(12) UK Patent Application (19) GB (11) 2 083 258 A

(21) Application No 8126556
(22) Date of filing
2 Sep 1981
(30) Priority data
(31) 8028391
(32) 3 Sep 1980
(33) United Kingdom (GB)
(43) Application published
17 Mar 1982
(51) INT CL^3 G08B 23/00
(52) Domestic classification
G4N 1P 4X 5A 6D1
6DX 6N 7A 7X EG GA
(56) Documents cited
None
(58) Field of search
G4N

(71) Applicant
Nuclear Power Company
Limited
1 Stanhope Gate
London
W1A 1EH
(72) Inventors
Brian Hills
Daniel Welbourne
(74) Agents
H V A Kirby Esq
Central Patent
Department
The General Electric Co
Ltd
Hirst Research Centre
Wembley
Middlesex

(54) Alarm systems

(57) An alarm system includes a computer 20 arranged to analyse various alarm conditions of apparatus (e.g. a nuclear power plant) to determine which alarms result from the prime causes of a number of alarms which may be present. The prime cause alarms are displayed on a visual display unit 32 and the presence of subsidiary alarms is indicated by group alarm lamp on a group alarm panel 34. The operator may request a display of all alarms present in a particular group.

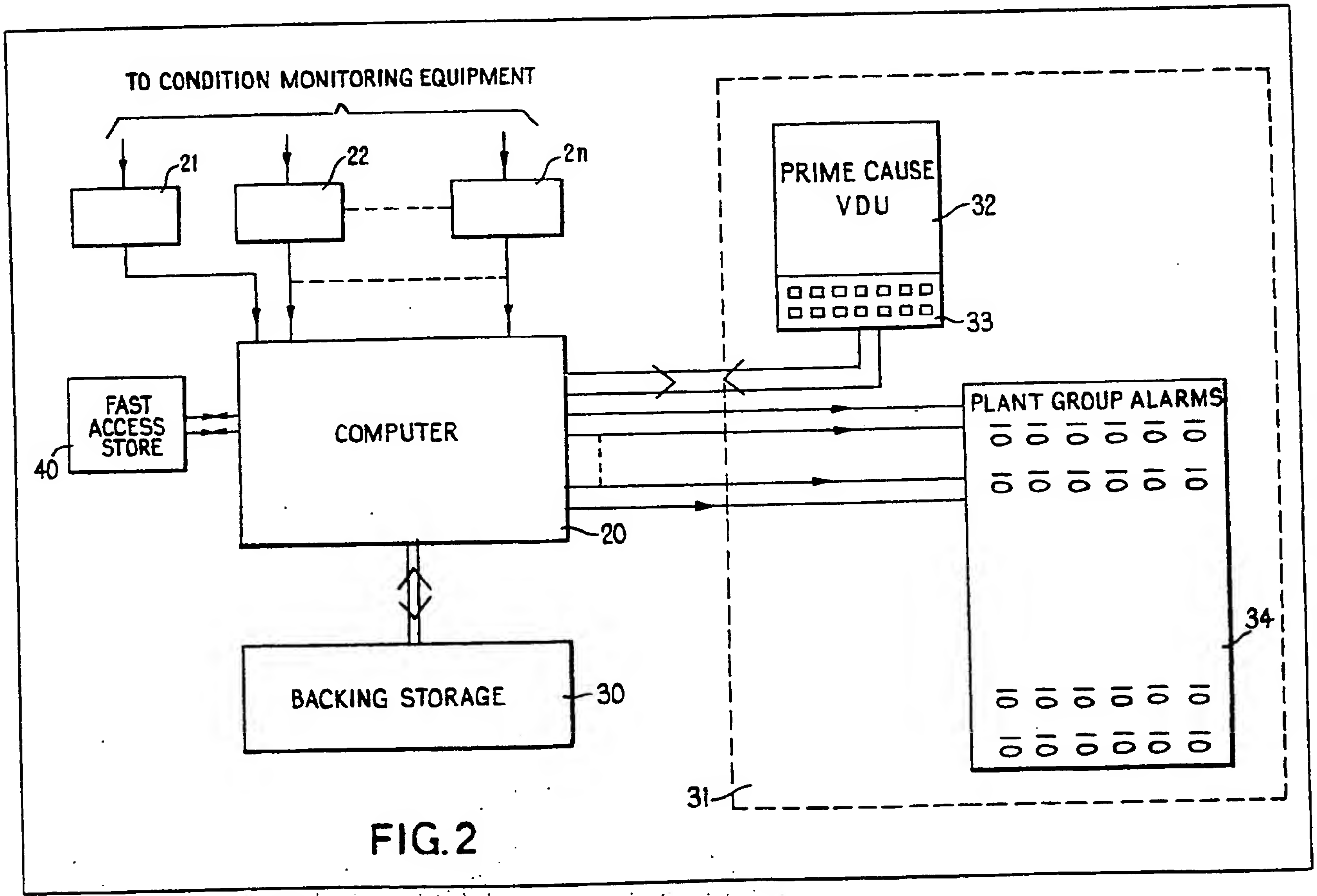

FIG. 2

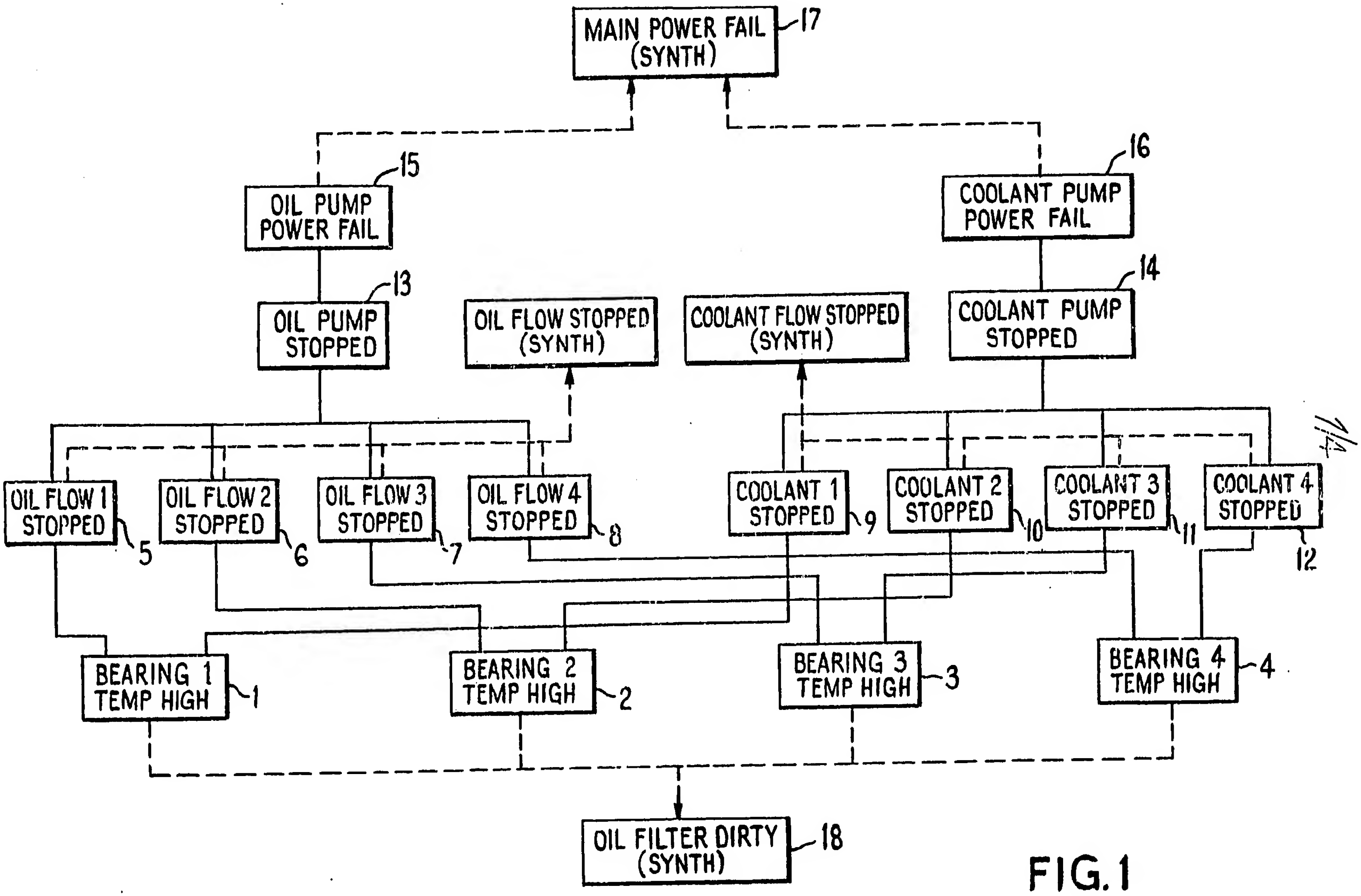
1/4
MAIN POWER FAIL (SYNTH)
17
OIL PUMP POWER FAIL
15
COOLANT PUMP POWER FAIL
16
OIL PUMP STOPPED
13
OIL FLOW STOPPED (SYNTH)
COOLANT FLOW STOPPED (SYNTH)
COOLANT PUMP STOPPED
14
OIL FLOW 1 STOPPED
5
OIL FLOW 2 STOPPED
6
OIL FLOW 3 STOPPED
7
OIL FLOW 4 STOPPED
8
COOLANT 1 STOPPED
9
COOLANT 2 STOPPED
10
COOLANT 3 STOPPED
11
COOLANT 4 STOPPED
12
BEARING 1 TEMP HIGH
1
BEARING 2 TEMP HIGH
2
BEARING 3 TEMP HIGH
3
BEARING 4 TEMP HIGH
4
OIL FILTER DIRTY (SYNTH)
18

FIG.1

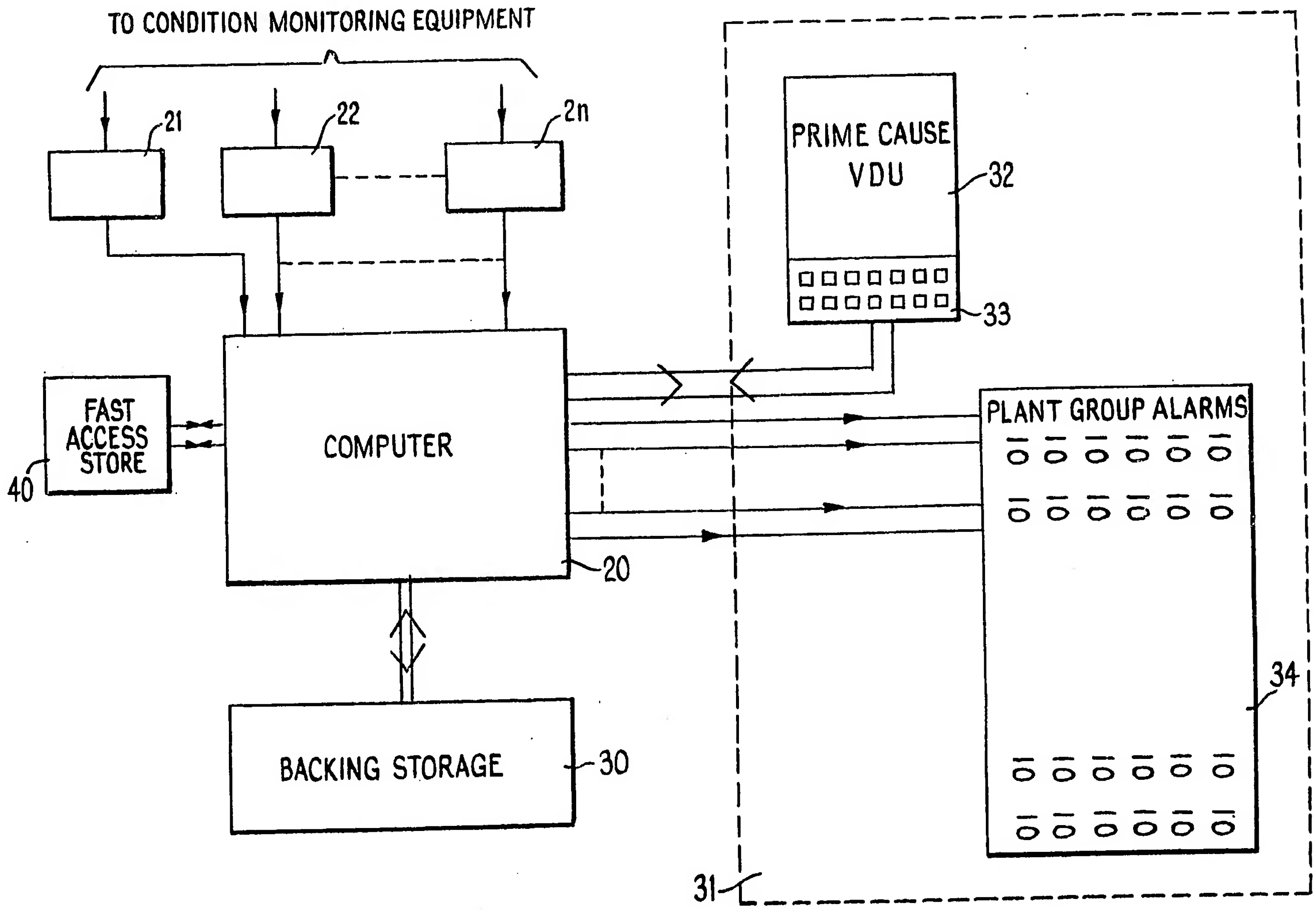
TO CONDITION MONITORING EQUIPMENT
21
22
2n
PRIME CAUSE VDU
32
33
FAST ACCESS STORE
40
COMPUTER
20
PLANT GROUP ALARMS
10 10 10 10 10 10
10 10 10 10 10 10
10 10 10 10 10 10
10 10 10 10 10 10
34
BACKING STORAGE
30
31

FIG. 2

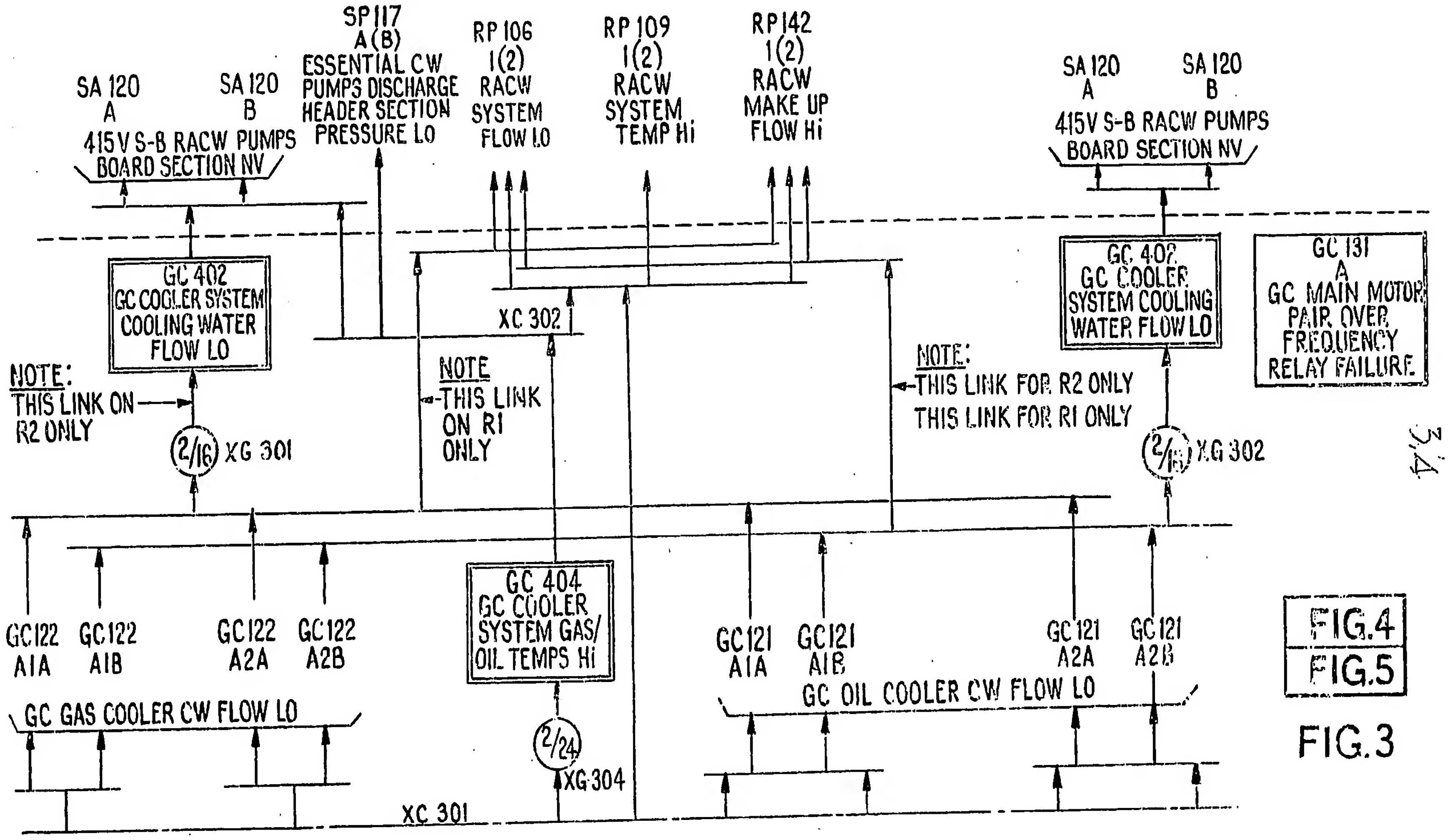

FIG.4

FIG.4
FIG.5

FIG.3

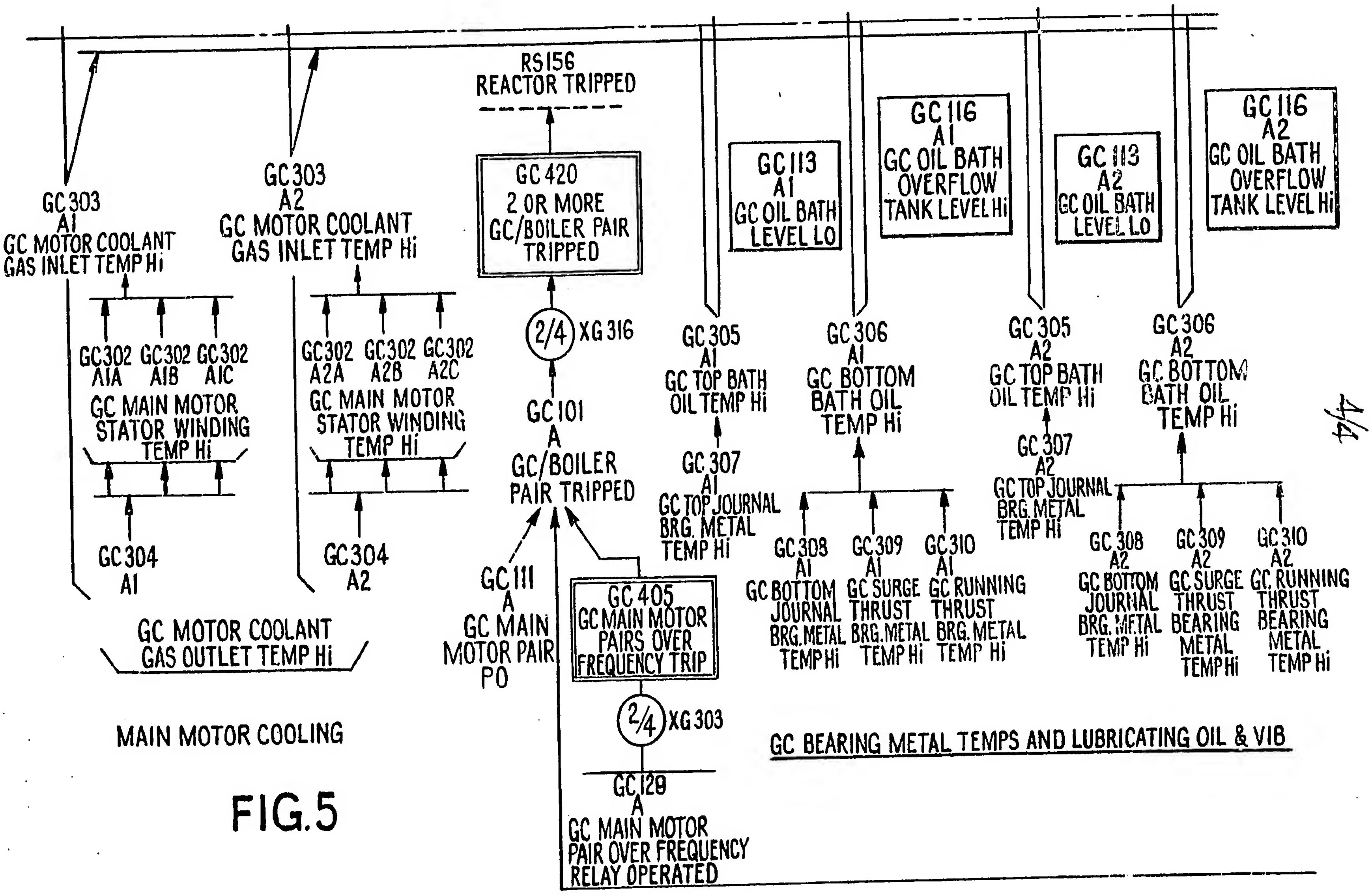
GC 303
A1
GC MOTOR COOLANT
GAS INLET TEMP Hi
GC 303
A2
GC MOTOR COOLANT
GAS INLET TEMP Hi
RS156
REACTOR TRIPPED
GC 420
2 OR MORE
GC/BOILER PAIR
TRIPPED
GC 113
A1
GC OIL BATH
LEVEL LO
GC 116
A1
GC OIL BATH
OVERFLOW
TANK LEVEL Hi
GC 113
A2
GC OIL BATH
LEVEL LO
GC 116
A2
GC OIL BATH
OVERFLOW
TANK LEVEL Hi
GC302 GC302 GC302
A1A A1B A1C
GC MAIN MOTOR
STATOR WINDING
TEMP Hi
GC302 GC302 GC302
A2A A2B A2C
GC MAIN MOTOR
STATOR WINDING
TEMP Hi
2/4
XG 316
GC 101
A
GC/BOILER
PAIR TRIPPED
GC 305
A1
GC TOP BATH
OIL TEMP Hi
GC 306
A1
GC BOTTOM
BATH OIL
TEMP Hi
GC 305
A2
GC TOP BATH
OIL TEMP Hi
GC 306
A2
GC BOTTOM
BATH OIL
TEMP Hi
GC 307
A1
GC TOP JOURNAL
BRG. METAL
TEMP Hi
GC 307
A2
GC TOP JOURNAL
BRG. METAL
TEMP Hi
GC 304
A1
GC 304
A2
GC 111
A
GC MAIN
MOTOR PAIR
PO
GC 405
GC MAIN MOTOR
PAIRS OVER
FREQUENCY TRIP
GC 308
A1
GC BOTTOM
JOURNAL
BRG. METAL
TEMP Hi
GC 309
A1
GC SURGE
THRUST
BRG. METAL
TEMP Hi
GC 310
A1
GC RUNNING
THRUST
BRG. METAL
TEMP Hi
GC 308
A2
GC BOTTOM
JOURNAL
BRG. METAL
TEMP Hi
GC 309
A2
GC SURGE
THRUST
BEARING
METAL
TEMP Hi
GC 310
A2
GC RUNNING
THRUST
BEARING
METAL
TEMP Hi
GC MOTOR COOLANT
GAS OUTLET TEMP Hi
2/4
XG 303
GC 129
A
GC MAIN MOTOR
PAIR OVER FREQUENCY
RELAY OPERATED
MAIN MOTOR COOLING
GC BEARING METAL TEMPS AND LUBRICATING OIL & VIB

FIG.5

synthetic alarms which are detected by logic analysis of the alarms which may be present in the group.

Subsidiary information, such as references to sections of an instruction manual, may also be held in the store.

When an alarm analysis for a particular group is either operator requested or is required in response to automatic analysis as hereinafter stated the plant group data for the respective group is located from the backing store 30 and is transferred to the fast access store 40.

A threading organiser programme now threads the data in the group through appropriate standard sub-routines of the computer 20.

The principle subroutines provided are titled ANALYSISGROUP, FETCH, LINK, DISPLAY and GROUP. The functions of each of these subroutines is as follows: The subroutine ANALYSISGROUP: *n* calls the data for group *n* from the backing store 30 to the fast access store 40 of the computer 20.

FETCH: alarm no. The FETCH subroutine examines the respective data word (as defined by the data called from the backing store) relating to the alarm number to determine whether the monitored condition is an alarm.

If the condition is normal (i.e. not an alarm) the programme proceeds to the next FETCH or if all alarms of this group have been examined to the next ANALYSISGROUP.

If an alarm is present a LINK or DISPLAY subroutine, dependent on the position of the alarm in the alarm tree will be entered.

LINK: alarm No. The LINK subroutine examines the respective data word (as defined by the data called from the backing store) relating to the alarm number to determine whether the alarm condition is present. If the higher order alarm condition is not present exit from the LINK subroutine is to either a further LINK or a DISPLAY subroutine. If the alarm condition is present exit from the LINK subroutine will be a subsequent FETCH or to the next ANALYSISGROUP.

GROUP: 'm': list 'p' synthetic alarm no. The GROUP subroutine is used to raise a synthetic alarm if a number 'm' of alarms of a subgroup of the main group is present. The alarm numbers of each member of the subgroup are held in a list 'p' which will have been transferred from the backing store by the ANALYSISGROUP subroutine. If 'm' or more of the alarms in list 'p' are present a DISPLAY subroutine is entered to display the synthetic alarm defined by the synthetic alarm number on the prime cause VDU 32. Exit from the GROUP subroutine is to a further GROUP subroutine or to a DISPLAY subroutine.

FETCH and LINK subroutines may exit to a GROUP subroutine.

The data for FETCH and LINK subroutines may include a system parameter to prevent the subroutine being entered when the check being made is not on the particular system.

Preparation of the data for each group may be more readily understood by consideration of following examples.

Referring to Figs. 4 and 5 when assembled as shown in Fig. 3 the alarm tree shown is for a gas circulator (GC) system of a nuclear power station having two reactors (R1 and R2).

The lower left hand corner of Fig. 4 includes an alarm statement GC motor coolant gas outlet temperature hi. The data for this alarm would show that GC304A1 is "GC A1 Motor Coolant Gas outlet temperature high" and that the alarm may be subsidiary to the alarms GC302A1A, GC302A1B, GC302A1C and GC303A1.

The threading organiser programme interprets this data through the subroutines as:—

FETCH: GC304A1

LINK: GC302A1A

LINK: GC302A1B

LINK: GC302A1C

LINK: GC303A1

DISPLAY: GCA1 MOTOR COOLANT GAS OUTLET TEMP HIGH.

The threading of the data as shown occurs if none of the alarms GC302A1A, GC302A1B, GC302A1C or GC303A1 is present and that GC304A1 is present. This being the case GC304A1 is the highest order alarm present and is displayed as the prime cause.

If one of the higher order alarms is present the threading of data through the LINK subroutines ceases and the threading organiser proceeds to thread data relating to the next alarm. The higher order alarm will subsequently be analysed in its own right and may then be displayed as the prime cause alarm.

Thus if GC302A1B is also in the alarm condition and assuming GC303A1 not to be so when the threading of data for GC302A1B occurs a prime cause display of "GC A1 MOTOR TEMP HIGH" will be displayed. Therefore the operator is led to the cause of the outlet temperature being high rather than the effect of the motor temperature being high.

Considering a more complex piece of analysis for the gas circulator gas cooling water flow as shown in the top left of Fig. 5 the threading organiser will thread data for this alarm:

FETCH: GC122A1A

LINK(R1): RP1061

LINK(R1): RP1421

GROUP:2: LIST 1 : GC402

DISPLAY: GCA1A GAS COOLER CW FLOW LOW.

List 1 will comprise GC122A1A

GC122A1B

GC122A2A

GC122A2B

Thus if GC122A1A is in the alarm condition, RP1061 of reactor 1 (LINK(R1)) (reactor cooling water system flow low) and RP1421 of reactor 1 are checked. If neither of the high order alarms are present then associated gas cooler cooling water flow alarms CG122A1A, GC122A1B, CG122A2A, GC122A2B are checked and if any two or more of these four alarms are present (GROUP:2) the synthetic alarm "GC402 GC cooler system cooling water flow low" is displayed on the prime cause VDU 32.

It will be appreciated that separating the scanning and analysis of the alarms rather than attempting to analyse each alarm as it arises, prevents the computer being swamped by making major demands on the backing store and waiting for the appropriate data to be transferred.

All alarms may be displayed to the operator but the principle faults are also made readily apparent.

In the absence of a specific request from the operator for an analysis of a particular group the computer 20 may be arranged to call for an analysis of each group in turn at periodic intervals so that the operator is kept informed of the prime causes of all the alarm conditions present in the system.

Since the computer is also capable of inputting various conditions such as the opening or closing of manually operable valves the operator may by use of the keyboard 33 request an analysis of a suitable plant state under fault conditions.

The threading organiser may be used to thread respective data through the same subroutines to analyse the current plant state and advise the operator on corrective procedures.

Accidents at various power stations have brought out the importance of correct preventative action when alarms initially appear, and of the importance of the coincidence of two or three fault states which of themselves, individually, result only in a correct operation of standby plant or in a reduction of plant integrity in a designed and individually acceptable manner.

As a particular example consider the restraints on operation in a nuclear plant which must be imposed in order to ensure continued availability of post-trip cooling, in the event of major hazards, for example, cable fires or coolant circuit breach.

Typically, four diesel driven fire fighting pumps may be provided for a station and operation may continue safely with one pump not available, but an increasing hazard exists if a pump outage is prolonged. If two pumps are not available, then within a period (say 2 hours) the station should be shutdown even if no fire exists, for reasons of prudence.

A gas cooled reactor typically has 4 boiler circuits, each with a gas circulating blower driven by a main motor, and by an auxiliary pony motor used at shutdown. Post-trip, at least one boiler must be available – where availability is defined by an actual requirement, such as follows:–

1a) The pony motor supply is available.

1b) The pony motor control supply is available.

1c) The pony motor control equipment is available.

1d) The pony motor protection has not operated

1e) Associated Gas circulator Bearing Temperatures are not excessive.

and

1f) An associated circulator inlet guide vane operating Fast Motor is available.

The unavailability of any of the above is indicated by the presence of an accompanying alarm.

Non-alarm operating constraints include:–

1g) An associated Pony Motor Mode Selector Switch is selected to the Auto Start position;

1h) A 415v Gas Circulator Board bus section switch is available whenever a Pony Motor/Boiler Unit within the same sub-set is not available;

1j) one 3.3 kV/415V Gas Circulator Transformer is available in each sub-set;

1k) An associated Emergency Feed Header Discharge Valve is fully open;

1l) an associated Economiser Isolating Valve is fully open;

1m) an associated Start-up Feedwater Regulator Valve is fully open;

1n) control equipment providing close action of the associated Boiler Stop Valve is available;

1o) associated Steam Dump Valve control equipment is available;

1p) automatic mode of control is selected for use on the Steam Dump Valve Control System. Selection of the manual mode of control is indicated by an alarm;

1q) the Steam Dump Valve Control Equipment is not on test. Equipment on test is indicated by an alarm; and

1r) Steam Dump Pressure Demand is within predetermined limits of the required value for use post-trip.

Operating restraints involved on boiler pairs can be expressed on the basis of two separate sets of boilers – say set one comprising Boilers A and B and set 2 comprising Boilers C and D.

For safety purposes (as an example):

2a) not more than one boiler must be unavailable within each set of a reactor at power for a period in excess of 1 hour unless orderly shutdown of the reactor is initiated;

2b) The unavailability of one boiler in either set is undesirable and should not be allowed to persist for long periods because if a fire should affect one set the circulator motor post-trip run on protection could affect the other set. Operation on three gas circuits should be initiated if the situation has not been improved after 4 hours, to reduce the probability of an available boiler unit being lost as a result of failure to trip a main motor breaker;

2c) The integrity of a boiler is attained by the use of redundant power supplies etc. Where one boilder unit of a set is unavailable and there is not a full complement of essential supplies available to the other unit or unavailability of changeover units, orderly shutdown of the reactor shall be initiated if the situation cannot be corrected within a period of 4 hours;

2d) The System integrity relies upon the availability of a fully connected Emergency Feed Header. It is undesirable for the header valves (either manual or automatic) to be closed. If a boiler is unavailable (say in set 2) the automatic or manual valve associated with the header section feeding the set 1 boilers should not be closed for more than 12 hours; or

2e) The unavailability of one boiler in one set coexisting with the unavailability in the other set of a Gas Circulator Transformer should not be allowed to persist for more than 8 hours.

The above restraints can be represented by a combination of alarm grouping and of truth tables. These in turn can be expressed by means of alarm analysis data and interpreted in the manner already described. The coincidence of operation of alarms may be used to generate appropriate alarms, and display a phrase including a time limit. A time delay subroutine may be included so that an additional alarm is displayed after the appropriate delay.

In the case of the above example, "boiler not available" alarms (1A, 1B, 1C, 1D for each boiler) must be derived by a GROUP subroutine involving 1(a) to 1(r) above, initiated as described if any of 1(a) to 1(r) are in the unacceptable state.

The backing store data to check the acceptability of the plant in respect of operating restraints 2(a) and 2(b) may be used by the threading organiser thus:

LIST R1R2: Boiler A; Boiler B; Boiler C: Boiler D;
LIST R1: Boiler A; Boiler B.
LIST R2: Boiler C: Boiler D.
GROUP: 2: LIST R1: SHUTDOWN ALARM
GROUP: 2: LIST R2: SHUTDOWN ALARM
GROUP: 1: LIST R1R2: ISOLATE ALARM
FETCH: SHUTDOWN ALARM
DISPLAY: TWO BOILERS FAILED—SHUTDOWN WITHIN 1 HOUR
FETCH: ISOLATE ALARM
LINK: SHUTDOWN ALARM
DISPLAY: BOILER FAILURE—ISOLATE WITHIN 4 HOURS

Thus when alarm analysis is carried out in the automatic mode the threading organiser threads the data through the provided subroutines first using the GROUP subroutine to determine whether both boilers (GROUP: 2) of either set (LIST R1/LIST R2) are unavailable. If this is the case the subroutine enters the shutdown alarm in the fast access store 40 and the backing store 30.

If any one of the four boilers is unavialable (GROUP:1) an isolate alarm is generated.

If the shutdown alarm is present the prime cause visual display unit 32 will display "TWO BOILERS FAILED— SHUTDOWN WITHIN 1 HOUR".

In this case the isolate alarm is treated as a subsidiary alarm. If the isolate alarm is present without the shutdown alarm the prime cause visual display unit 32 will display "BOILER FAILURE—ISOLATE WITHIN 4 HOURS".

The example above illustrates the principle for analysing plant states. The remaining operating restraints may be derived in a similar manner.

CLAIMS

1. An alarm system comprising a computer, first display means for displaying prime cause alarm information, further display means for displaying subsidiary alarms which are dependent upon at least one associated alarm displayed on the first display means, the status of each condition being monitored by the computer being presented at an input of the computer in digital form and being read by the computer at periodic intervals, the computer having at least one data word for each of the conditions being monitored and being arranged at each reading of a condition to compare the current status of said condition with the previous status of the condition as indicated by its respective stored data to determine when a change of status of the condition occurs and if the change of status indicates that the condition is an alarm to determine to which one of *n* groups of alarms the alarm belongs, and to activate a respective one of *n* warning means of the further display means associated with the particular group of

alarms the computer also being arranged periodically to consider each alarm with respect to any other alarms to determine whether the alarm is a prime cause or is an alarm resulting from another cause and to display each said prime cause alarm on the first display means.

2. An alarm system as claimed in Claim 1 in which said first display means is a visual display unit.

3. An alarm system as claimed in Claim 2 in which the computer is arranged to cause each prime cause alarm to be displayed as a phrase or sentence on the visual display unit.

4. An alarm system as claimed in Claim 3 in which the computer is also arranged to cause the visual display unit to display a reference to further information which is available for at least some of the displayed prime cause alarms.

5. An alarm system as claimed in any preceding claim in which the computer is also arranged periodically to consider predetermined groupings of the conditions being monitored and, if more than a specified number of one of said predetermined groupings are in an alarm state without a higher order alarm relating to a monitored condition being present, to cause the first display means to display a prime cause alarm determined from said grouping.

6. An alarm system as claimed in any preceding claim in which the computer is also arranged periodically to consider the operational capability of parts of the apparatus being monitored, to determine the acceptability of continued operation of the apparatus if some parts of the apparatus are not available for use and, if continued operation of the apparatus is unacceptable to cause said first display means to display an appropriate message.

7. An alarm system as claimed in Claim 6 in which the computer is also arranged to determine, in dependence on the parts of the apparatus which are not available for use and by consideration of the probability of further parts of the apparatus becoming unavailable, the probability of continued operation of the apparatus becoming unacceptable within a calculated period and to cause the first display means to display a warning message including said caculated period.

8. An alarm system as claimed in any preceding claim including a keyboard for use by an operator to request the computer to display on the first display means the titles of all of the alarm conditions present in one of said groups of alarms.

9. An alarm system as claimed in Claim 8 in which the computer is also arranged to respond to a keyboard request for an analysis of one of said groups of alarms.

10. An alarm system substantially as hereinbefore described with reference to the accompanying drawings.

Printed for Her Majesty's Stationery Office
by Burgess & Son (Abingdon) Ltd.—1982.
Published at The Patent Office, 25 Southampton Buildings,
London, WC2A 1AY, from which copies may be obtained.